ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ІЄРАРХІЧНОГО КОДУВАННЯ У ФОРМАЛЬНИХ ГРАМАТИКАХ

С. В. Тіхонов, д. т. н. В. С. Ситніков

Національний університет «Одеська політехніка»
Україна, м. Одеса
od.sergii.tihonov@gmail.com

Розглядаються питання кодування інформації на рівнях мережевих інтерфейсів в комп'ютерних системах Інтернету речей, ланки вразливості та загрози захисту персональних даних. Аналізуються архітектурні моделі Інтернету з точки зору сумісності мережевих інтерфейсів. Пропонуються принципи ієрархічного кодування даних на рівнях мережевих інтерфейсів у формальних граматиках, які ускладнюють перехоплення даних в каналах зв'язку та підвищують захист комп'ютерних систем Інтернету речей.

Ключові слова: комп'ютерна система, захист інформації, кодування даних, формальна граматика, інтерфейс.

Термін «Інтернет речей» (IoT) вперше було використано для підключених до пакетної мережі фізичних об'єктів з сенсорними датчиками (1999 р.). Наразі IoT означає перехід до якісно нового етапу еволюції Інтернету, сервіси якого поширюються на безліч пристроїв, сенсорів і приводів. Сенсорні мережі доступу IoT наближені до масового користувача інтернет-послуг, і тому цей напрямок домінуватиме у тій частині Інтернету, яка стосується мереж доступу. Подальший розвиток Інтернету у сегментах концентрації та розподілу трафіку сформульовано в концепції NGN (Next Generation Networks), що інтегрує різноманіття типів даних і мережевих послуг на основі IP. Ядром Інтернету є транспортна система оптичних ліній на основі високошвидкісних когерентних оптичних комунікацій. Також активно впроваджуються глобальні супутникові мережі мобільного зв'язку типу Starlink. Кожен з вказаних аспектів має свої особливості та виклики [1].

В цій роботі розглядаються питання кодування інформації на рівнях мережевих інтерфейсів комп'ютерних систем Інтернету речей (КС-IoT), для яких одним з найбільших викликів є захист персональних даних. Ланками вразливості КС-IoT є радіоканали, програмне забезпечення контролерів, пристрої розподілу трафіку. Кіберзахист КС-IoT ускладнюється великим обсягом даних і документів різного типу, кожен з яких є потенційним джерелом загроз. Так, файли типу "exe" та "com" можуть містити вірусні програмні закладки (bookmarks), які самі по собі не є носіями вірусу, натомість посилаються на Web-ресурс, що його містить. PHP-програми Web-серверів здатні приховувати "чорні двері" (backdoors) — зловмисний програмний код, що скасовує нормальні процедури автентифікації доступу; в результаті, зловмисник отримує віддалений контроль інформаційних ресурсів. Витоки інформації та шкідливі втручання можуть здійснюватися прихованими каналами взаємодії через вірусні коди у файлах типу "jpeg". Детальний огляд потенційних загроз в мережах IoT і розширена бібліографія наведені в [2, с. 7].

Різноманіття загроз і методів протидії, а також зростаючі ризики кібератак у сучасному світі потребують подальших теоретичних і практичних досліджень проблеми кіберзахисту телекомунікаційних каналів IoT з урахуванням особливостей мережевих інтерфейсів на різних рівнях архітектури комп'ютерних систем. Одним із перспективних напрямків в теорії кодування та захисту інформації є представлення цифрових потоків послідовністю команд у ієрархічних формальних граматиках, рівні якої відповідають інтерфейсам обраної моделі взаємодії відкритих систем в мережі IoT. Це дозволяє розділити складну задачу наскрізного кодування на окремі складові частини.

Метою цієї роботи є обґрунтування принципів захисту інформації у комп'ютерних системах Інтернету речей на основі ієрархічного кодування даних у формальних граматиках на рівнях архітектурної моделі мережевих інтерфейсів.

Функціональну структуру комп'ютерних мереж відображують "архітектурними моделями" апаратно-програмних мережевих інтерфейсів, пристроїв і процесів в них. Еталонна 7-рівнева модель

OSI Міжнародної організації по стандартизації ISO описує взаємодію “відкритих систем” — абстрактних інтерфейсів (1978—1980 рр.). За фактом, світова Мережа має 4-рівневу архітектуру стеку протоколів TCP/IP Цільової групи з розвитку Інтернету IETF (1978—1989 рр.). Моделі OSI та TCP/IP розвивались паралельно, однак у намаганні вичерпного опису мережі модель OSI не отримала підтримку розробників Інтернету. Поява додатків реального часу виявила обмеження моделі TCP/IP, створеної для передачі файлових даних. У 2004 р. ITU анонсував 3-рівневу модель мереж наступних поколінь NGN для підтримки якості обслуговування. Сенсорні мережі IoT створили потужні цифрові потоки телеметрії, непритаманні мережам TCP/IP. Невдовзі з’явились нові еталонні моделі IoT:

— *ITU-T Y.2060*-2012 (4 рівні: пристрої, мережа, сервіси, додатки);

— *IoT World Forum Reference Model*-2014 (7 рівнів: пристрої, інтерфейси, туманні обчислення, акумуляція даних, агрегація даних, додатки, бізнес-процеси);

— *NIST SP 800-183*-2016 (4 рівні: сенсори, агрегатори, комунікації, управління; ця модель сфокусована на безпеці комп’ютерних систем);

— *Industrial IoT (IIoT) Reference Architecture*-2022 (3 рівні: кінцеві пристрої, IIoT- платформа, людські та цифрові користувачі).

Аналіз моделей свідчить про незавершеність архітектури Інтернету. Фахівці вважають сумісність телекомунікаційних мереж (interoperability) однією з ключових проблем 21 століття [3].

Враховуючи моделі Інтернету та технології телекомунікацій (Ethernet, TCP/IP), представимо IoT-інтерфейси об’єктами 7-рівневої формальної граматики G^7:

1) “каліграфія” — зображення символів алфавіту (лінійне кодування);

2) “орфографія” — написання слів (блокове кодування);

3) “синтаксис” — написання речень (фреймів канального рівня);

4) “пакетування” повідомлення в окремі “сторінки” файлу (пакети);

5) “комплектація” — формування файлу повідомлення з пакетів;

6) “криптозахист» — шифрування даних;

7) “семантика” — інтерпретація даних (мережеві додатки рівня L7 OSI).

Рівні G^7 є самостійними граматиками 1-го рангу $G^1{}_k \in \{G^1{}_k\}$. В процесі передавання даних передбачається стохастичний вибір поточних граматик для інтерфейсів різних рівнів з множини $\{G^1{}_k\}$. Для управління вибором поточної граматики можна застосувати приховані “метакоманди”, замасковані у потоці повідомлень.

Впровадження ієрархічного кодування з динамічною комутацією граматик дозволить ускладнити перехоплення та змістовну інтерпретацію даних у процесі передачі по каналах зв’язку розподіленої комп’ютерної системи Інтернету речей. Практична реалізація вказаних принципів і отримання чисельних оцінок їхньої ефективності є предметом наших подальших досліджень.

.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Жураковський Б.Ю., Зенів І.О. *Технології інтернету речей*. Київ, КПІ, 2021, 271 с.

2. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches. *Sensors*, 2022, № 22, p. 1335.

3. Teixeira de Sousa P., Stuckmann P. Telecommunication Network Interoperability. *Telecommunication systems and technologies*, 2009, vol. II, 422 p.

S. Tikhonov, V. Sytnikov

Information protection principles for Internet of Things computer systems based on hierarchical coding in formal grammars

The authors consider information coding issues at the network interface levels in Internet of Things computer systems, vulnerability links, and threats to personal data protection. Internet architectural models are analyzed for interfaces interoperability. The principles of hierarchical data coding in formal grammars are proposed at the network interface levels to hinder communication channels tracking and increase computer systems protection in the Internet of Things.

Keywords: computer system, information protection, data coding, formal grammar, interface.